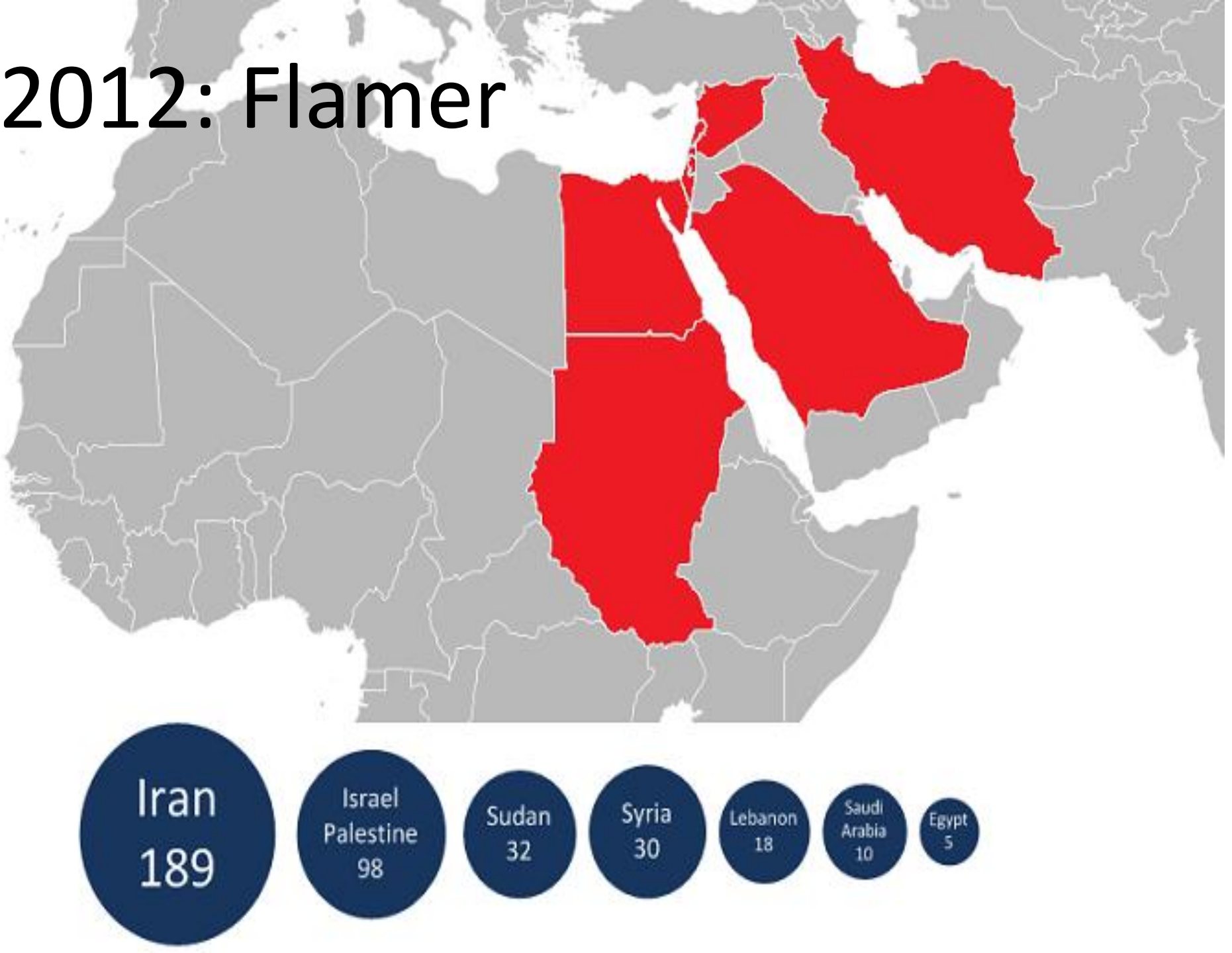
Securing Critical Information Infrastructures and Services

Evangelos OUZOUNIS
Head of CIIP & Resilience
ENISA

2011: Attacks on governments

2012: Flamer


Iran
189
Israel
Palestine
98
Sudan
32
Syria
30
Lebanon
18
Saudi
Arabia
10
Egypt
5

Cyber Exercises, the Big Three

- Europe's first ever international cyber security exercise, 2010

- First ever EU-US exercise, 2011. Work with Comm. & MS to build transatlantic cooperation

- Cyber Europe 2012. Developed from learning in 2010 & 2011 exercises. Involves MS, private sector and EU institutions. Highly realistic exercise, Oct 2012

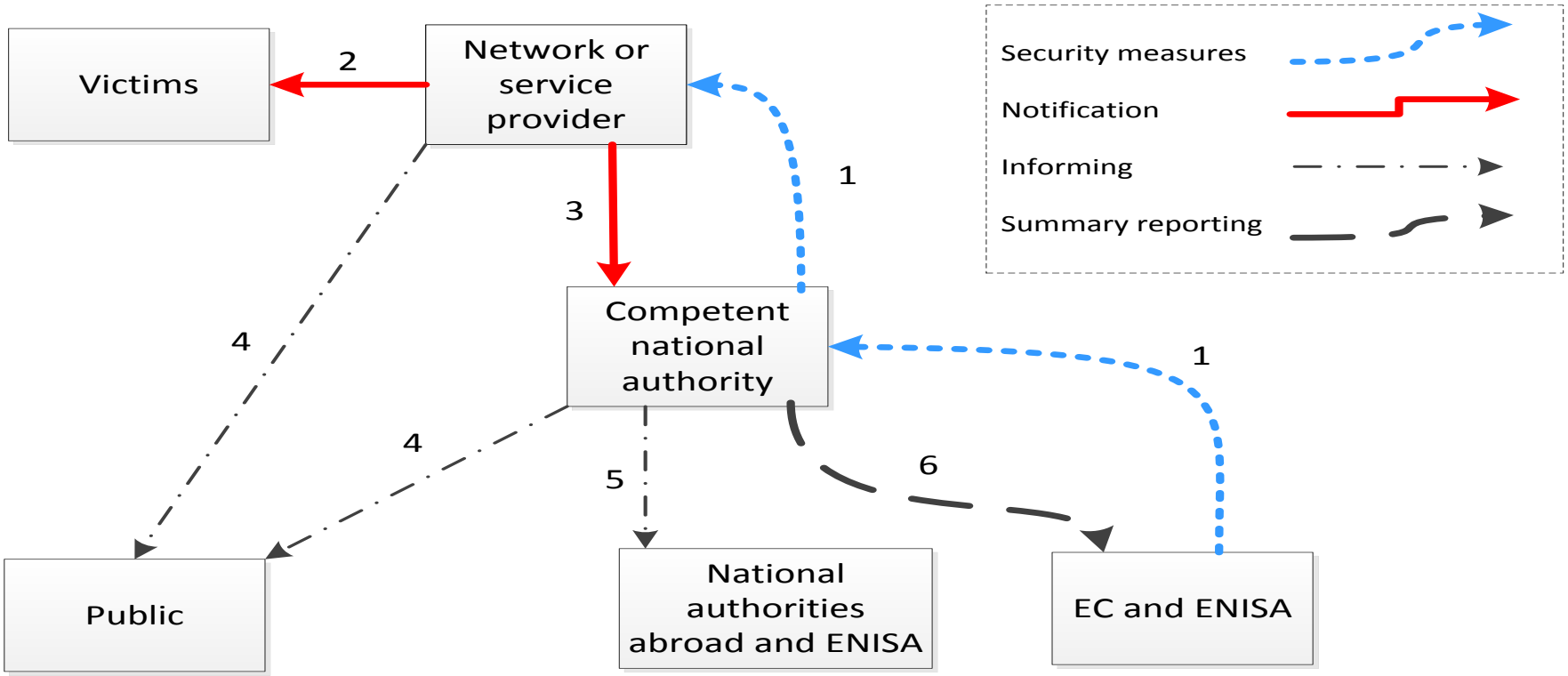
2nd Pan - European Cyber Exercise

Cyber Europe 2012 – media coverage

- More than 100 news stories so far – Europe, plus USA
- Most online and broadcast media
- Follow-up media requests still coming in (@ 08/10/2012)

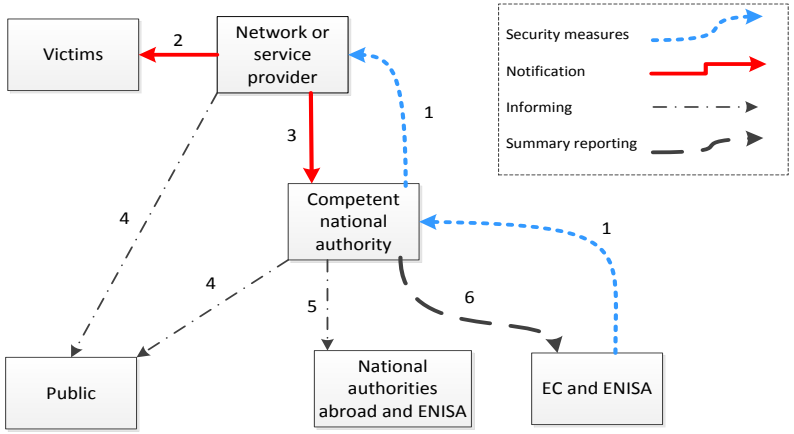
Overview of Article 13a

- Appropriate security measures for e-comms providers
- Incident reporting for e-comms providers

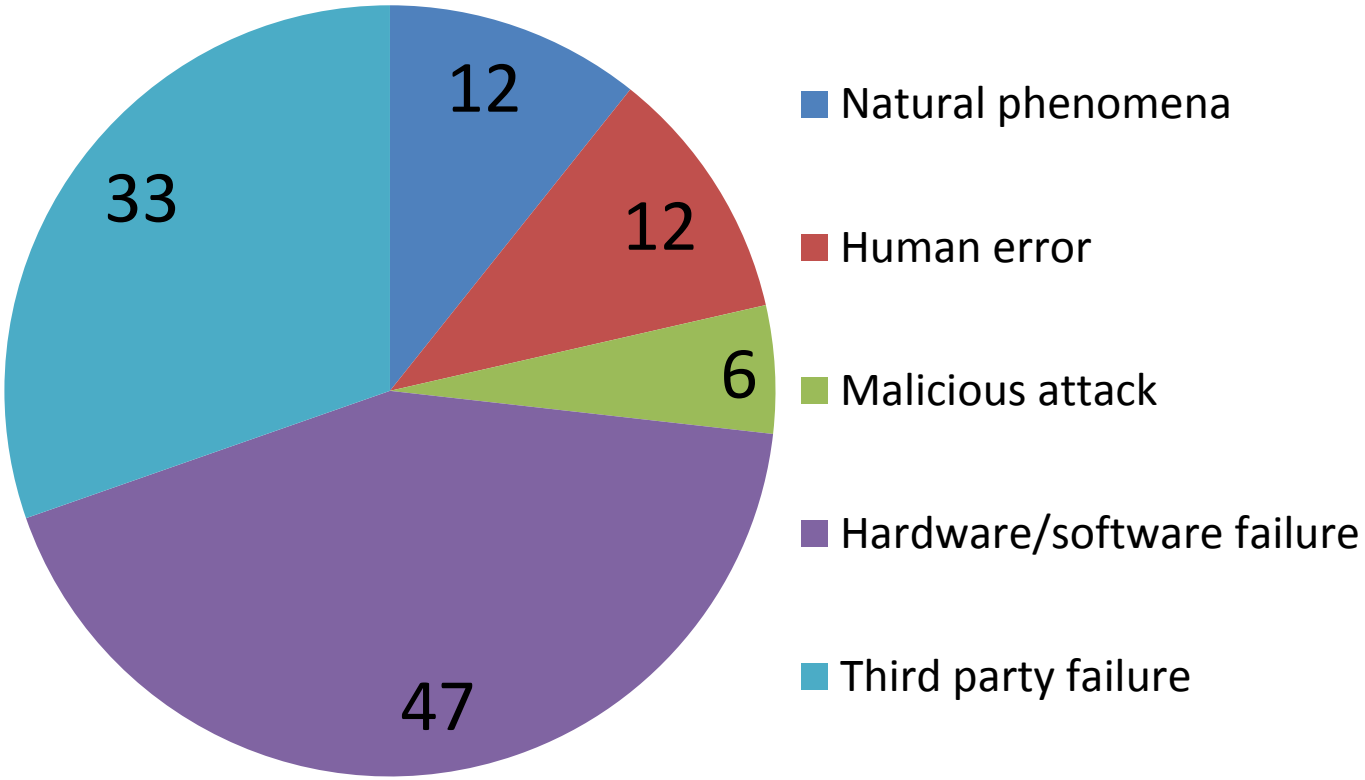


Article 13a - Incidents 2011

- 51 incidents from 11 countries, 9 countries without significant incidents, 9 countries with incomplete implementation
- Most incidents
  - affect mobile comms (60%)
  - are caused by
    - hardware/software failures (47%)
    - third party failures (33%),
    - natural disasters (12%)
- Many involve power cuts (20%)
- Natural disasters (storm, floods, et cetera)
  - often cause power cuts, which cause outages
  - cause incidents lasting an average of 45 hours
- Next report spring 2013, expected around 500 incident reports



Root Causes of 2011 incidents



EP3R - Public Private Partnership for Resilience

- provide a platform for information sharing and stock taking of good policy and industrial practices
- discuss public policy priorities, objectives & measures
- improve coherence and coordination of policies for security and resilience in Europe;
- 3 Working Groups
  - WG 1: Interdependencies of ICTs to critical Sectors
  - WG 2: Baseline requirements for security and resilience of electronic communication networks
  - WG 3: Coordination and cooperation mechanisms
    - Botnets
    - Pan European exercise

Cloud Computing

Objectives for Cloud Computing at ENISA

- Help governments and businesses to leverage the cost benefits of cloud computing, with due consideration of security requirements and new risks
- Improve transparency on security practices to allow informed decisions
- Create trust and trustworthiness by promoting best practice and assurance standards

Report defines minimum baselines for:

- Comparing cloud offers
- Assessing the risk to go Cloud
- Reducing audit burden and security risks

http://www.enisa.europa.eu/act/application-security/rm/files/deliverables/cloud-computing-risk-assessment

Smart Grid Security

- **ENISA recommendations include:**
  - Establishing of clear regulatory and policy framework on smart grid cyber security at national and EU level – currently missing.
  - The EC, with ENISA, MS, and private sector, should develop minimum set of security measures based on existing standards and guidelines
  - EC and MS authorities should promote security certification schemes for the entire value chain of smart grids components, including organisational security

www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

Smart Grid Security

- **ENISA recommendations include:**
  - Establishing of clear regulatory and policy framework on smart grid cyber security at national and EU level – currently missing.
  - The EC, with ENISA, MS, and private sector, should develop minimum set of security measures based on existing standards and guidelines
  - EC and MS authorities should promote security certification schemes for the entire value chain of smart grids components, including organisational security

www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA-smart-grid-security-recommendations

Contact us, follow us

resilience@enisa.europa.eu

twitter

twitter.com/enisa_eu

website

www.enisa.europa.eu